



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|-------------------------------|---------------------|------------------|
| 09/622,047 | 08/23/2000 | Alexandr Andreevich Moldovyan | P65855US0 | 4150 |

136 7590 06/20/2005

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

EXAMINER

LANIER, BENJAMIN E

| ART UNIT | PAPER NUMBER |
|----------|--------------|
|----------|--------------|

2132

DATE MAILED: 06/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/622,047

Applicant(s)

MOLDOVYAN ET AL.

Examiner

Benjamin E Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 May 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. The amendment filed 05 May 2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: transforming the subkey with the operation of transposing bits.

Applicant is required to cancel the new matter in the reply to this Office Action.

Response to Arguments

2. Applicant's arguments filed 05 May 2005 have been fully considered but they are not persuasive.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., conversion of data subblocks which are then used to convert subkeys) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Claims recite the conversion of the subblocks, but only require that the subkeys be transformed. The claims do not specifically require the subblocks to be used to actively convert the subkeys.

3. Applicant's argument that Den Boer does not disclose transforming the subkey with the operation of transposing bits, which changes initial sequence of the subkey bits and depends on the j-th subblock prior to performing two-place operation on the I-th subblock is not persuasive

Art Unit: 2132

because Den Boer discloses that the two subkeys (K1, K2) are input into a cipher function with two subblocks of a message block (M1, M2) to produce an enciphered message block (T) (Col. 5, line 26 – Col. 6, line 21 & Figs. 5-7). During the cipher function the bits of the subkeys are transposed (Figure 7).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Den Boer, U.S. Patent No. 6,298,136. Referring to claim 1, Den Boer discloses a non-linear cryptographic method wherein a message block that is to be encrypted is segmented into two sub blocks (Col. 5, lines 26-31), which meets the limitation of breaking down a data block into $N \geq 2$ sub blocks. An encryption key is generated and subsequently split into two sub keys (Col. 5, lines 45-47), which meets the limitation of generating an encryption key in the form of a set of sub keys. The two sub keys and the two sub blocks can be split further, and each sub key is associated with a sub block (Col. 5, lines 47-51). Each sub block is processed separately by a cipher function with its associated sub key to produce an encrypted message block (Col. 5, line 51 – Col. 6, line 21). The result of the rounds of processing yield transposed sub keys (Figure 7), which meets the limitation of converting in turn said sub blocks by performing a two-place operation on the sub block and the sub key, characterized by the transforming the sub key with the operation of

Art Unit: 2132

transposing bits, which changes initial sequence of the subkey bits and depends on the j-th sub block prior to performing the two-place operation on the i-th sub block where $i \neq j$.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. Claims 2-4 rejected under 35 U.S.C. 103(a) as being unpatentable over Den Boer, U.S. Patent No. 6,298,136 as applied to claim 1 above, and further in view of Coppersmith, U.S. Patent No. 6,192,129. As per claims 2 and 4, as described in the teachings applied above with respect to claim 1, Den Boer discloses a method for block encryption of discrete data comprising steps a-d. Den Boer does not expressly disclose either an operation of permuting subkey bits or a substitution operation performed on a subkey as being the conversion operation of step d. However, Coppersmith et al discloses such operations as prior art (Coppersmith et al - column 22, lines 1-5 and 44-45 and column 23, lines 15-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Den

Art Unit: 2132

Boer to include either the operation of permuting subkey bits or the substitution operation performed on a subkey as the j-th subblock-dependent conversion operation as per the teachings disclosed in Coppersmith et al. One of ordinary skill in the art would have been motivated to do so in order to generate multiple distinct keys for the multiple rounds of the encryption algorithm (Coppersmith et al - column 2, lines 11-13).

As per claim 3, as described in the teachings applied above with respect to claim 1, Den Boer discloses a method for block encryption of discrete data comprising steps a-d. Den Boer does not expressly disclose an operation of cyclic offsetting subkey bits as being the conversion operation of step d. However, Den Boer discloses such an operation as prior art (column 2, lines 1-15). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Den Boer to include the operation of cyclic offsetting subkey bits as the j-th subblock-dependent conversion operation as per the disclosed prior art. One of ordinary skill in the art would have been motivated to do so in order to generate multiple distinct keys for the multiple rounds of the encryption algorithm (Coppersmith et al - column 2, lines 11-13).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

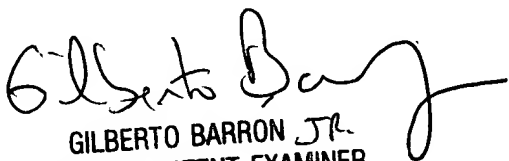
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100